

PORTLAND COMMUNITY COLLEGE RELIES ON UNIFIED ACCESS CONTROL FOR WIRELESS LAN ACCESS



Industry: Education

Challenges:

- Add network and applications access control to the campus-wide wireless LAN used by more than 90,000 people a year
- Minimize administrative burden on IT and administrative staff
- Continue to meet community needs while limiting use of the wireless network to people affiliated with the college or community

Selection Criteria: As an established customer of Juniper Networks for security solutions, Portland Community College chose Juniper Networks Unified Access Control to control access to its WLAN and network applications.

Network Solution:

- Juniper Networks IC4000 Controller and UAC agent
- Juniper Networks SSG140 Secure Services Gateway

Results:

- Deployed access control for its on-campus wireless network, accessible to more than 90,000 individual users
- Allowed staff, students and community members associated with the college to access and use the wireless network while maintaining strong network security
- Minimized effort to deploy and maintain network access control by leveraging its existing investment in network equipment and its existing business processes

More than 86,000 people a year enroll in Portland Community College (PCC) in Oregon to earn associate's degrees, advance their careers or just learn something new. PCC serves the residents of this fast-growing area in the Pacific Northwest from three campuses and five work centers across the metropolitan Portland area.

Like many educational institutions, PCC maintains a delicate balance between openness and security. Students, faculty and staff can use the college's wireless network to communicate and work from common areas. When wireless LAN service was rolled out more than two years ago, anyone physically on the campus could access and use the wireless network. "Community colleges in general have a very open environment," says Greg Malone, technical services division manager at Portland Community College. "We have a mission to serve the community as well."

Challenge

But within that spirit of openness, it is the IT department's duty to protect the college's computing and network resources. "Our goal was to maintain a private wireless network," says Malone. "On the wired side, we have a private network designed for PCC staff, students and visitors who are here to conduct business. We wanted the same controls on the wireless network."

To achieve the delicate balance between accessibility and control, PCC deployed access control for its wireless LAN. Students, faculty and community members can use the wireless service at their convenience, while individuals who have no affiliation with PCC are prevented from accessing and using PCC's wireless LAN. Controlling wireless access and limiting use to authorized users not only improves network and application security, but it also preserves the network bandwidth for legitimate users.

Selection Criteria

Working under tight deadlines, PCC went from evaluation to deployment in just three months. Malone and his IT team examined the alternatives for authentication on wireless networks, and invited the leading technology vendors to present their solutions. PCC ultimately selected Juniper Networks

IC Series to control access to and the use of its wireless network. PCC has a long history with Juniper, having deployed several of the company's networking and security solutions, including core routers and firewalls.



“Network access control is a technology that’s new to our environment, and based on our previous experiences with Juniper and its solutions, we felt that UAC was market-worthy and that we could trust them,” says Malone. “We have prior experience with Juniper and a good relationship with them.”

“Based on our previous experiences with Juniper solutions, we felt that the UAC products were market-worthy and we could trust them.”

Greg Malone,
Technical Services Division Manager, Portland Community College

Solution

Today, some 90,000 students, faculty and staff logon and authenticate to PCC’s wireless network—which spans more than 350 access points across the PCC campus—via Juniper’s UAC. PCC deployed a IC4000 and UAC agent, which is the policy manager at the heart of the UAC. The SSG140 appliances serve as the enforcement points for the wireless network’s access control deployment.

The IC4000 is the UAC’s hardened, centralized policy management server that collects and centralizes user authentication, endpoint security state and device location information. Once user credentials are validated and security state established, the Infranet Controller creates and implements an appropriate, dynamic access policy for each user/session, and propagates that policy to enforcement points (such as the Juniper SSG140s that PCC deployed) throughout the network.

The SSG140s are designed to deliver a perfect mix of routing, security and LAN/WAN connectivity for regional and branch offices. They provide a complete set of Unified Threat Management (UTM) security features including stateful firewall, IPSec VPN, IPS, antivirus (includes anti-spyware, anti-adware and anti-phishing), anti-spam and Web filtering.

Results

Supporting 90,000 users with limited IT resources means that ease of deployment and administration for the UAC solution at PCC was paramount. At the same time, the college also wanted to establish a relationship with users prior to their use of the wireless network.

PCC uses the SSG140s as enforcement points at the network edge and utilizes UAC’s agent-less mode for endpoint assessment and user identification. This solution ensures the continued enforcement of user/device authentication and network security policies while eliminating the need to deploy and manage clients on individual computers. “UAC’s agent-less solution works well,” says Malone.

Account creation and provisioning had to be highly automated, or it could easily be an overwhelming administrative process. “We have a very large and transitory population, and managing student accounts in a non-automated way wasn’t feasible,” says Malone. “It was extremely important to have an automated process.”

Accounts are automatically created for currently enrolled students, faculty and staff based on integration with the college’s ERP system. They logon to the college’s wireless network using the same credentials they would use to access other PCC electronic resources.

Then Malone had to tackle the challenge of guest user access. “We leveraged an existing process that we used for parking permits to create wireless guest accounts. The guests are automatically sent their user name and password,” says Malone. To create guest accounts with a minimum of hassle, PCC leveraged a Web-based application that’s used for guest parking permits. Community members wishing to use the college’s WLAN can go to a library or resource center where administrative staff can set up their account using the same Web-based system.

Supporting events was particularly challenging—having administrative staff create potentially hundreds of individual guest user accounts for an event wasn’t practical. To eliminate the need to create individual guest accounts, PCC decided to use a shared user ID and password that’s unique to each event.

With the IC Series in place, PCC can now easily enforce access policies on its wireless network. Students and guests have only Internet access, while staff has access to a PCC portal, based on their role. Behind the scenes, users are authenticated to an LDAP database. "Wireless access is transparent to the users," says Malone.

Wireless access had been in the free and clear for several years at PCC, so adding authentication caused a small stir at first, but students and staff quickly settled in to the new routine. PCC added network access control in the summer of 2007, and when 47,000 students arrived for the fall 2007 term, everything went smoothly. "We're very pleased with IC4000," says Malone. "User acceptance went smoothly and there has been no impact to our IT support resources."

Next Steps and Lessons Learned

PCC's IT team invested heavily in upfront planning for access control, which paid off handsomely in a smooth rollout. "We thought through the process so that we could establish accounts in the least disruptive way and leverage processes that we've been using for other projects. That effort made the rollout seamless," says Malone. "Most of the struggles were with the process, not the technology."

"If you're considering network access control at your organization, do your due diligence on the project," Malone advises fellow IT managers considering a similar rollout. "Upfront planning is very important. Success invariably comes down to smart project management processes."

PCC is continuing to rollout wireless networking across the campus with in-building and outdoor coverage next on its to-do list. For the next phases of its UAC rollout, PCC is planning on giving employees and students access to additional resources from the wireless network and deploying UAC in High Availability mode for improved business continuity.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate And Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. "Engineered for the network ahead" and JUNOSE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

